Lab Assignment 3 – Vulnerabilities and Malware

Task 1: Introduction to port scanning

1. What is a port scan?

   A port scan is a way for systems administrators to find or what ports are open and what ports are closed on a system. This process is normally automated with port scanning tools like NMAP or Nessus.

2. What is the difference between a TCP full connection port scan and TCP half-open scan?

   The difference between a full connection and half open connection is in the full connection the port scanner will complete the full 3-way handshake, this process is much slower than the half connection method. The half connection method sends the syn and waits for the syn-ack packet to come back be then never responds to it. This makes it much faster as fewer packets need to be sent.

3. Using the common ports list from Wikipedia for reference, name three ports, that if found open, could be useful to an attacker to gain access to the system? Why?

   Port 23 Telnet, this port should never be left open. It is unsecure and everything done on it is sent in plain text. It also provides remote shell capability making it a very powerful attack vector for attacker.
   Port 22 SSH can also be a good attack vector if not configured correctly. It offers remote shell access and can also be susceptible to Brute for and credential reuse. It can also be used for privilege escalation and lateral movement.
   Port 53 DNS Can be useful if left open depending on what services it is running. It can be used for attacks like Cache poisoning and spoofing, and with this port open you can look for vulnerable software like BIND and PowerDNS for example.

4. What is nmap?

   Nmap/Zenmap are commonly used port scanning tools used to scan for open ports on a network. They automate the process and make port scanning much easier and faster than could be done by hand.

5. Using the Nmap Outputs provided in FSO, list the ports found open for the Windows and Linux operating systems that were scanned with Nmap.

   Windows Machine Ports: 135, 139, 445, 5040, 7680, 49664, 49665, 49666, 49667, 49668, 49669, 49719
   Linux Version: OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9

Deliverable: **Submit your answers to the above questions as part of your lab write-up.**

Task 2: Introduction to vulnerability scanning

1. What is a vulnerability scan?

   A Vulnerability scan helps an organization identify, assess, and quantify vulnerabilities in their environment. This can also be used by attackers to find potential vulnerabilities that they may be able to exploit.

2. What is the difference between an authenticated and unauthenticated scan?

   The Main difference between the 2 scans is that with an authenticated scan is more of an internal view as you have credentials to enter the system/network. This approach helps reduce false positives and gives a much deeper understanding of the potential vulnerabilities. An unauthenticated scan is a good way for organizations to get an "outside in" perspective so that they can see what an attacker can see and mitigate those risks. This method can produce more false positives so always confirm these results.

3. What are the three steps of the vulnerability scanning process as referenced in the article?

   Identify Vulnerabilities, Evaluate and Prioritize Vulnerabilities, Resolve Vulnerabilities.

4. Nessus, an enterprise vulnerability scanning product, enables enterprises to scan a variety of systems for vulnerabilities. Using the Nessus vulnerability scanning report from FSO, what is the IP address that has the most vulnerabilities? NOTE: This is not associated to the NMAP scans from Task 1.

   192.168.158.131

5. Based on the vulnerabilities listed for the IP address from question #4, what operating system do you think was being scanned? Note: Pay close attention to the findings (especially the critical findings)

   Linux, as it mentions Debian

Deliverable: **Submit your answers to the above questions as part of your lab write-up.**

Task 3: Introduction to endpoint protection (classically known as Anti-Virus)

6. What are the fundamental differences between legacy anti-virus software and modern "next generation" endpoint protection?

What makes this the “next generation” is the combined use of AI, behavioral detection, machine learning, exploit mitigation and cloud technology. With all these combined it help minimize setup time, system resource use and the time it takes to respond to zero days and keeping up to date.

7. Do you believe that modern endpoint protection would be more effective against today’s threats? Why or why not?

   I think that Modern endpoint protection is not the sole solution to rely on for modern threats. They should be used in a defense in depth solution. They are part of the solution, not the entire thing. They can help with detecting bad once it gets on your system but what you really want is for the bad to never get on the system in the first place. This can be accomplished with education for end users, correctly configuring network devices and hardening systems.

8. Do some research and list a few “next generation” endpoint protection vendors that are in the market today?

   CrowdStrike Falcon, SentinelOne Singularity, Microsoft Defender for Endpoint, Palo Alto Networks Cortex XDR, Threatlocker Endpoint Protection and Trend Micro Vision One.

References:

Endpoint Search:
https://www.google.com/search?q=what+are+some+next+generation+endpoint+protection+solutions&rlz=1C1RXQR_enUS1132US1132&oq=What+are+some+NExt+generation+Endpoint+protecion+solu&gs_lcrp=EgZjaHJvbWUqCQgBECEYChigATIGCAAQRRg5MgkIARAhGAoYoAEyBwgCECEYjwIyBwgDECEYjwLSAQoyNTcwOWowajE1qAIIsAIB8QUMg0hyHjxCKQ&sourceid=chrome&ie=UTF-8